

REMARKS

Claims 22, 23, 24, 25, 26, 28, 29 - 33 and 35 - 41 are pending. Claims 1 – 21, 27, and 34 have been cancelled. Claims 36 - 41 have been added. Claims 22, 23, 25, 28 - 32 and 35 have been amended. No new matter has been introduced.

Reexamination and reconsideration of the application are respectfully requested.

In the June 14, 2005 Office Action, the Examiner rejected claims 1 - 7, 8 - 13, and 14 - 21 under 35 U.S.C. § 101 because these claims recite a software program which is per se non-statutory subject matter. The applicants have cancelled claims 1 - 7, 8 - 13, and 14 - 21.

In the June 14, 2005 Office Action, the Examiner rejected claims 1 - 31 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 4,723,284 to Munck ("the Munck reference"). This rejection is respectfully traversed in so far as it is applicable to the presently pending claims.

Claim 29 distinguishes over the Munck reference. Claim 29, as amended, recites:

A hardware authenticity verification system, comprising:
a machine-readable storage medium; and
machine-readable program code, stored on the machine-readable storage medium, the machine-readable program code having instructions, which when executed cause a data processing device to:
create a digital signature of a hardware address of a hardware element installed in the data processing device;
store the digital signature of the hardware address of the hardware element in a memory element;
compare the digital signature of the hardware element to a known value; and
load device driver software onto to the hardware element only if the digital signature of the hardware element is the same as the known value.

The Munck reference does not disclose, teach, or suggest the hardware authenticity verification system of claim 27, as amended. The Examiner states that the Munck reference discloses that a hardware address is associated with a private key that is unique to the hardware and that cannot be accessed or used in another way. (*Office Action, page 6*). Specifically, the Munck reference discloses a public key network with a user terminal and a hardware authentication terminal, which are coupled by a communication medium. The user terminal is characterized by a public key and an associated private key and the private key is not derivable from the public key and is stored in the terminal in such a way that it cannot be accessed. (*Col. 2, lines 38 - 48*).

The authentication terminal 12 of the Munck reference authenticates that the user terminal is who it says it is. The authentication terminal 12 extracts the user terminal's public key from the authentication terminal 12 memory 44 and transfers the public key to the network. A controller 40 in the authentication terminal 12 directs a generator 42 to generate a plaintext message (M) which is transferred to the network 46. The authentication processing network 46 in the authentication terminal 12 generates a ciphertext message, using the public key, and transfers the ciphertext message to the user terminal 14 via a modem 48 and the communication medium. (*Col. 4, lines 1 - 10*). The user terminal 14 receives a message and under the control of its controller 20, the private key is retrieved from memory 26 and applied to the message to transform the message into a second plaintext message (M'). The user terminal 14 sends the second plaintext message to the authentication terminal 14 where the original plaintext message (M) is compared to the second plaintext message (M'). If the comparison indicates a match, an authentication signal is generated (from

the authentication processing network 46) indicating that the user terminal 14 is the desired user terminal. (*Col. 4, lines 11 - 26*).

The Munck reference also discloses the use of a software authentication terminal 60 which confirms that a remote user terminal 62, which includes a computer, is operating under the control of a specific software program. (*Col. 4, lines 37 - 40*). The software authentication terminal 60 inquires about the status of the user terminal 62. In response to the inquiry signal, user controller 80 initiates a checksum generator 86 and a state generator to generate a check sum signal (CS) and a state signal (S) representative of the state of that processor. A software authentication message generator provides a remote program signal (RP) representative of the two component signals (CS and S). The received RP signal is applied to a checksum / state comparator 72 in the software authentication terminal 60. The software authentication terminal 60 controller 66 generates corresponding checksum and state signals (CS' and S') which are combined to form a local program signal (LP). The LP signal is applied to the comparator 72 and if the LP signal and the RP signal match, the comparator 74 generates a confirmed status signal representative of confirming that the user terminal is operating under the control of the desired software program. (*Col. 5, lines 4 - 35*).

This is not the same as a hardware authenticity verification system, including instructions which when executed cause a data processing device to **create a digital signature of a hardware address of a hardware element installed in the data processing device and store the digital signature of the hardware address of the hardware element in a memory element.** The Munck reference does not disclose that a digital signal of a hardware address of a hardware element is generated.

Instead, the Munck reference discloses that the hardware of its disclosure, i.e., the user terminal or the authentication terminal, can be utilized to implement digital signing functions such as digital signing of a document. (*Col. 5, lines 55 - 61*). In other words, the Munck reference discloses that a digital signature of the public key or private may be implemented. There is no mention that a **hardware address of a hardware element stored in the data processing device is digitally signed**, as is recited in claim 29, because the Munck reference does not even discuss utilization of a hardware address nor does the Munck reference disclose utilization of a hardware address of a hardware element. Accordingly, claim 29, as amended, distinguishes over the Munck reference.

Claim 29, as amended, further distinguishes over the Munck reference. The Munck reference does not disclose a hardware authenticity verification system, including instructions, which when executed cause a data processing device to **compare the digital signature of the hardware element to a known value; and load device driver software onto to the hardware element only if the digital signature of the hardware element is the same as the known value**. In contrast, the Munck reference discloses either that 1) a plaintext message (M) is compared to a second plaintext message (M') or 2) that a remote signal (RS), which represents a remote checksum signal and status signal, is compared to a local signal (LS), which represents a local checksum signal and status signal. The Munck reference is also disclosing that this occurs in the authentication terminal and not the user terminal (the user terminal being akin to the claimed invention's data processing device). This is different than **comparing a digital signature of the hardware element to a known value**, as

recited in claim 29, which all takes place within one computer, i.e., within the data processing device. Further, there is no disclosure in the Munck reference that **device driver software is loaded onto the hardware element only if the digital signature of the hardware element is the same as the known value**. In contrast, in the Munck reference the software is already loaded on both the user terminal and the authentication terminal. Accordingly, claim 29, as amended, further distinguishes over the Munck reference.

Claim 22 recites limitations similar to claim 29, as amended. Accordingly, applicants respectfully submit that claim 22 distinguishes over the Munck reference for reasons similar to those discussed above in regard to claim 29, as amended.

Claims 23 - 26, 28, 30 - 33 and 35 depend, indirectly or directly, on claims 22 and 29, as amended. Accordingly, applicants respectfully submit that claims 23 - 26, 28, 30 - 33 and 35 distinguish over the Munck reference for the same reasons as those discussed above in regard to claim 29, as amended.

Claim 32 further distinguishes over the Munck reference. Claim 32 recites:

The hardware authenticity verification system according to claim 31, wherein the machine-readable program code includes instructions, which when executed cause the computer to **manipulate the hardware address of the hardware element that is stored in memory with a hash algorithm to generate the known value which is compared to the digital signature of the hardware element**.

The Examiner states that the Munck reference discloses the manipulating the number of hardware with a hash. (*Office Action, page 3*). The applicants do not see where in column 6 of the Munck reference that the Examiner believes the hash is disclosed. Assuming that the Munck reference does disclose the manipulating of a

number by a hash algorithm, the Munck reference does not disclose that a **hardware address of a hardware element** is manipulated utilizing a hash algorithm.

Accordingly, applicants respectfully submit that claim 32 distinguishes over the Munck reference.

Independent claim 36 distinguishes over the Munck reference. Claim 36 recites similar limitations to claim 29. Accordingly, claim 36 distinguishes over the Munck reference for reasons similar to those discussed above in regard to claim 29. Claim 36 further distinguishes over the Munck reference. Claim 36 recites:

A verification system, comprising:
a machine-readable storage medium; and
machine-readable program code, stored on the machine-readable storage medium, the machine-readable program code having instructions, which when executed cause a data processing device to:
create a digital signature of a hardware address of a network adapter installed in the data processing device;
store the digital signature of the hardware address of the network adapter in a memory element;
compare the digital signature of the network adapter to a known value; and
load device driver software onto the network adapter only if the digital signature of the network adapter is the same as the known value.

The Munck reference does not disclose the utilization of a hardware address of **a network adapter**. The Munck reference is referring to the utilization of a modem and not a **network adapter** and there is no disclosure in the Munck reference of any utilization of a network address. Accordingly, applicants respectfully submit that claim 36 further distinguishes over the Munck reference.

Independent claim 39 recites limitations similar to claim 36. Accordingly, applicants respectfully submit that claim 39 distinguishes over the Munck reference for reasons similar to those discussed above in regards to claim 36.

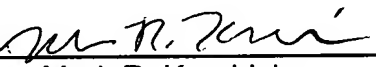
Claims 37 - 38 and 40 - 41 depend, indirectly or directly, on claims 36 and 39, respectively. Accordingly, applicants respectfully submit that claims 37 - 38 and 40 - 41 distinguish over the Munck reference for the same reasons as those discussed above in regard to claim 36.

Applicants believe that the pending claims are in condition for allowance, and a favorable action is respectfully requested. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Los Angeles telephone number (213) 488-7100 to discuss the steps necessary for placing the application in condition for allowance should the Examiner believe that such a telephone conference would advance prosecution of the application.

Respectfully submitted,

PILLSBURY WINTHROP SHAW PITTMAN LLP

Date: September 14, 2005

By: 
Mark R. Kendrick
Registration No. 48,468
Attorney for Applicant(s)

725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
Telephone: (213) 488-7100
Facsimile: (213) 629-1033